Data Breaches in Higher Education

Lori Coleman
Holy Family University, Philadelphia, Pennsylvania

Bernice M. Purcell, DBA
Holy Family University, Philadelphia, Pennsylvania

ABSTRACT

Data breaches are becoming more common in higher education. Data compromised in higher education breaches extend far past grades; personal and financial data are abundant at all institutions, and sensitive research data are stored at many large universities. The environment of openness and collaboration at colleges and universities, as well as the typical access of many portable devices make access easier for hackers and detection of unauthorized access difficult. The most common types of data breaches occurring in college and university systems are hacking and malware, unintentional disclosure, and portable device breaches.

Four universities cases of data breaches studied are Pennsylvania State University, University of Maryland, North Dakota State University System, and Butler University. Each of the universities experienced a major data breach. The breaches had many similarities, including remote access and for some the sophistication of the attack. All of the breaches were costly. College and university administrators need to be prepared for data breaches, including plans to secure against a breach and react to a breach. Best practices in security and communication of the polices establish preventive measures, while cyber insurance, timely notification, and free fraud protection are typical reactive measures available to college and university administrators.

Keywords: Data breach, higher education, breach prevention, breach reaction

INTRODUCTION

When the subject of hacking and data breaches in colleges and universities arises, people tend to think of students hacking into the network to adjust their grades to hide bad performance from their parents and future employers. However, recent data breaches at several universities have shown that student grades are not the main. Chabrow (2015) explains that university systems are seen as ideal targets for hackers since the systems contain sensitive personal data as well as an abundance of intellectual property from researchers. Chabrow describes the cyber-criminals infiltrating the institutional systems as well-funded and highly skilled perpetrators who have become brazen in their attacks. Nick Bennett, senior manager at Mandiant, told Reuters (Kumar, 2015) that cyber-attacks similar to the one at Penn State in 2015 are the new normal and that no company or organization is immune. The hacks are sophisticated, difficult to detect and often linked to international threat actors.

Colleges and universities have large amounts of data and are difficult to secure. Hackers have used several methods to hack higher educational institutions in the last couple of years from hacking and malware to skimming hardware and insider attacks. According to information from the massive database maintained by Privacy Rights Clearinghouse, 30 educational institutions experienced data breaches in 2014 alone. Five of the 30 higher educational institutions actually had larger data breaches than the notorious Sony Hack. (McCarthy, 2015) This paper examines data targets at universities, types of breaches to access the data, several recent university breaches and suggested actions to prevent such attacks.

WHAT ATTRACTS HACKERS TO COLLEGE AND UNIVERSITY DATA?

Educational institutions are seen as an "easy target" for cyber-attackers according to Tyler Shields, a security analyst at Forrester Research (Roman, 2014). Shields, who previously worked for Rochester Institute of Technology in New York, states that the culture of academic institutions is one of open communication and collaboration among students, staff, faculty members and research groups. The network users are highly mobile and are accustomed to networking and accessing the network whenever and wherever they are and on any device. The academic culture of openness and unencumbered access to content and data makes college and university networks extremely difficult to secure. The lax security allowing open access and the presence of cutting-edge academic research and content on the networks make educational institutions an attractive target for attackers (Roman, 2014).

In an article in InsideHigherEd.com (Straumshein, 2015), Chad Holmes, a chief security strategist with FireEye, makes similar statements about the culture of higher education and difficulties of securing their networks. Like Shields, Holmes said that it is the nature of universities which makes the networks tougher to secure. Holmes continues that universities are more difficult to secure than companies and government agencies due to the fact that faculty members and students demand more control of their data than do employees of companies and government agencies. While companies may distribute and control the devices that access corporate networks, people use a myriad of devices on college campuses to access data, which poses serious security risks. (Straumshein, 2015)

The sheer number of students, faculty, staff, and alumni make university databases an attractive target for hackers. Personally identifiable information (PII) and financial information such as credit card numbers for such a large number of individuals is very attractive. Greenberg

(2014) explained that PII and financial data are attractive to hackers since the information can be bought and sold in bulk, often quite cheaply. A structured and rather sophisticated market for PII has been developed. Greenberg continues that university databases contain underlying personal data for thousands, if not millions, of people. If information for a single credit card sells for $10, hacking into a database where thousands of them can be acquired at one time can be extremely lucrative.

The cutting edge research being done at universities is also a rich target for hackers. Chambrow (2015) reasons that large research universities would be great targets for hackers who are sponsored by or sell to other governments, including China. Many large universities research and develop sensitive, cutting-edge technology. Rebecca Herold, a security expert, offered her opinion that intellectual property seemed to have been the target of the Penn State University hack. Her reasoning was based on the fact that the original target of the PSU hack was the College of Engineering (Chambrow, 2015)

COMMON TYPES OF DATA BREACHES IN HIGHER EDUCATION

The categories of data breaches that are most common in higher education are hacking or malware, unintended disclosure, and portable device breaches. Hacking or malware is defined by the Privacy Rights Clearinghouse as entry into a system by an outside party or data loss due to malware or spyware. Unintended disclosure is the exposure of sensitive or personally identifiable information through website posting or mishandled e-mail, fax, or mail (items sent to the wrong party). Portable device breaches are those due to portable devices such as laptops, tablets, cell phones, memory devices, etc. that are lost, discarded improperly, or stolen. Researchers at the ECUCAUSE Center for Analysis and Research (ECAR) determined that 36% of breaches were committed by hacking or malware, 30% by unintended disclosure, and 17% by portable device breaches (Grama, 2014).

FOUR UNIVERSITY CASES

Pennsylvania State University

Pennsylvania State University (Penn State) was hacked twice in a three year period. Penn State hired Mandiant, the forensic unit of cyber-security firm FireEye Incorporated after the early 2015 breach was discovered. Mandiant's forensic research determined that the first attack took place in September 2012, with the second being mid-2014. Mandiant confirmed that at least one of the two attacks was carried out by a "threat actor" based in China (Kumar, 2015). Ken Westin, senior security analyst for the IT security firm Tripwire, says intellectual property was the likely target of the Penn State hack, given that the hackers targeted the engineering department. Westin continued by mentioning that collaboration between higher education and private industry to commercialize research are common in large research universities. The university-industry collaboration combined with the fact that higher education generally lacks the resources to develop a strong security posture makes universities a target for sophisticated attackers. Westin says that like many large research universities, Penn State has a number of multimillion dollar contracts with the Defense Department. Getting information about Defense Department projects might prove attractive to China as well as other governments and may tempt the governments to subsidize hackers (Chabrow, 2015)

Penn State representatives claim the attackers did not steal any proprietary or sensitive research information despite the fact that the unauthorized network access was undetected for more than two years. Penn State officials also state that attackers did not steal any PII such as credit cards numbers or Social Security numbers of students, faculty, or staff (Donahue, 2015). Donahue questions Penn States' claim by noting that the school's admissions office notified 18,000 individuals that a file containing their Social Security numbers in plain text existed on affected machines. Donahue further questioned how hackers could fail to steal anything of value when the hackers had more than two years of access to the Penn State network.

As a result of the breach Penn State administrators required all network users to change passwords. Penn State also instituted additional layers of authentication before allowing access to the network. The university estimates that roughly $2.85 million has been spent responding to the attacks. More than $450,000 was paid to external experts to further secure the network and the remaining $2.4 million was spent replacing infected hardware (Donohue, 2015)

University of Maryland

University of Maryland (UMD) personnel discovered a data breach in February of 2014. Brian Voss, vice president and chief information officer at UMD, said officials believe whoever accessed the database duplicated the information. The data beached included names, Social Security numbers, dates of birth, and university identification numbers for 309,079 people affiliated with the school on the College Park and Shady Grove campuses (Svitek & Anderson, 2014). Voss described the breach by explaining the attackers essentially "made a Xerox of it and took off" (Svitek & Anderson). Voss continued that his biggest concern was the sophistication of the attack. The hacker or hackers must have had a "very significant understanding" of how the school's network and data are designed and protected (Svitek & Anderson). Voss further stated that the security breach appeared to be in contrast with typical university attacks in which "someone left the door open" creating an easy opportunity for any hacker (Svitek & Anderson). Continuing the open door metaphor, Voss explained that the hackers needed to pick through several locks when attempting to access the data. Voss had considered the network and data at UMD to be secure (Svitek & Anderson, 2014)

A former contractor of UMD claims in April 2014 that he had warned the university executives of the network vulnerabilities, but his information was ignored. David Helkowski, former contract worker for UMD, said he hacked into scores of databases in the school's computer system. To prove his point Helkowski posted the university president's private information online to draw attention to security problems (Hedgpeth & Anderson, 2014). As a result of the breach, University of Maryland provided free credit monitoring for one year to anyone whose information was compromised.

North Dakota University

Notifications posted to the North Dakota University System (NDUS) website indicated that the university's information technology service provider, Core Technology Services, was tipped off to an intrusion on Feb. 7, 2014. The university immediately shut down the affected server which was accessed using compromised credentials (Greenberg, 2014). North Dakota University System notified more than 290,000 former and current students and roughly 780 faculty and staff that their personal information may have been at risk. The information compromised by an unauthorized party who gained access to one of the NDUS servers included such things as Social Security numbers. The nature of the data breach was not revealed. The breach may have been committed by hacking or by unintentional disclosure of access credentials. (Greenberg, 2014).

North Dakota University System was the most pro-active and re-active of the universities studied regarding response to the data breach. The university proactively employed a service to continually monitor institutional networks for unauthorized access. Reactively, NDUS enhanced other security measures to ensure a similar incident does not occur. The enhanced measures include initiating stronger intrusion detection, revalidating each individual user, and developing a taskforce to address accessing data securely. Like other similar breaches, all impacted individuals were offered a free year of identity protection service (Greenberg, 2014).

Butler University

California law enforcement officials contacted administration at Butler University on May 28, 2014 to alert the administrators of an investigation involving a suspect who had in his possession a flash drive containing the personal information of certain Butler University employees (Roman, 2014). The data breach affected more than 163,000 students, faculty, staff and alumni at Butler University in Indianapolis, Indiana. Forensic investigators determined that the breach occurred between November 2013 and May 2015 (Roman, 2014). The investigators could only narrow the breach down to an eighteen month period and until the flash drive was found, the university administrators were not aware data breach had occurred. Remote hacking was suspected in the case. In response to the data breach, those affected by the breach were offered one year of free credit monitoring services (Roman, 2014).

PREPARING FOR AND REACTING TO DATA BREACHES

"Unfortunately, we now live in an environment where no computer network can ever be completely, 100 percent secure" a Penn State representative shared (Chabrow, 2015). The PSU representative further stated that on the average day the PSU university computer system repels more than 22 million overtly hostile cyber-attacks from around the world (Chabrow, 2015). Colleges and universities need to have plans in place to prepare and to react to data breaches.

Beaudin (2015) makes several recommendations as to how colleges and universities can prepare for a data breach and react to a breach when one occurs. Preparation for a data breach is an important part of an overall information security plan. Plans for reacting to a breach acknowledges that breaches are likely to occur and details in advance how to mitigate damage and costs due to the breach.

Information technology administrators need to ensure that information technology best practices and security policies are adopted and communicated (Beaudin, 2015). Personnel handling data need to know how data are collected, stored, and protected. Responsible personnel need to know their role in incident response in case of data vulnerability (Beaudin). All people on campus handling data need to know their role in data safety, including administrators, faculty, staff, researchers, and students. Practices and policies include password, authentication, access, and portable devices issues. Communication is a crucial element of a successful plan – everyone needs to know his or her particular role in preventing a breach and reacting to a breach.

Personnel can encrypt sensitive data. Data encryption prevents anyone without a decryption key from being able to read the data (Beaudin, 2015). Data accessed by anyone without the decryption key will be useless. Hackers accessing and taking encrypted data would not be able to use or sell this data.

Administrators can consider cyber insurance to offset cost of a data breach (Beaudin, 2015). O'Neil (2015) includes costs of professionals such as forensics consultants and lawyers and services such as call centers, identity-protection, and credit-check services as expenses related to a data breach. Total cost estimates of university breaches have reached several million dollars for a single breach (Beaudin, 2015; O'Neil, 2015).

The two main means of reacting to a data breach are timely notification and free fraud protection (Beaudin, 2015). Responsible administrators need to inform affected employees and students once a breach is detected and compromised data identified. Free fraud protection is typically offered to identified victims; the cost is a major expense of the data breach.

CONCLUSION

Data breaches of higher educational institutions are serious threats to university data and PII of faculty, staff, students, and alumni. Hundreds of thousands of people have had their personal information and intellectual property stolen in the attacks studied. The amount of personal, financial, and other sensitive data available in college and university networks is extremely attractive to hackers. The nature of the higher educational culture of openness and collaboration as well as the number of personal devices allowed and supported on university campuses makes the institutional networks difficult to secure. College and university administrators need to employ best practices to secure data, including plans to prevent data breaches and steps to take once a breach has been detected. Educating the user base regarding the importance of security and the role of users in making the network more secure is part of a good security plan. The institutional staffs need to be vigilant in authenticating network users and monitoring for unauthorized access.

REFERENCES

Beaudin, K. (2015). College and university data breaches: Regulating higher educaiton cybersecurity under state and federal law. *Journal of College and University Law, 41* (3), pp. 657 - 694. http://www.nacua.org/securedocuments/nonsearched/jcul/41_jcul_657.pdf

Chabrow, E. (2015, May 15). China blamed for Penn State breach - Hackers remained undetected for more than two years. from *databreachtoday.com*: http://www.databreachtoday.com/china-blamed-for-penn-state-breach-a-8230

Dark Reading. (2013, May 22). The right most common cCauses of data breaches. from *DarkReading.com*: http://www.darkreading.com/attacks-breaches/the-eight-most-common-causes-of-data-breaches/d/d-id/1139795?

Donohue, B. (2015, May 18). Penn State Off-line Following Advanced Two-Year Cyberattack., from *ThreatPost.com*: https://threatpost.com/penn-state-offline-following-advanced-two-year-cyberattack/112872

Grama, Joanna, et. al. (2014). Just in time research; Data breaches in higher education. *EDUCAUSE.* https://net.educause.edu/ir/library/pdf/ECP1402.pdf

Greenberg, A. (2014, March 06). North Dakota University System hacked, roughly 300K impacted. from *SCmagazine.com*: http://www.scmagazine.com/north-dakota-university-system-hacked-roughly-300k-impacted/article/337181/

Hedgpeth, D., & Anderson, N. (2014, April 10). Ex-contractor says he hacked into U-Md. databases to alert others to security flaws. from *WashingtonPost.com*: http://www.washingtonpost.com/local/crime/former-contractor-calls-himself-whistleblower-in-exposing-security-problems-at-u-md/2014/04/10/7312699e-c0b3-11e3-b195-dd0c1174052c_story.html

Kumar, D. K. (2015, May 15). Penn State says College of Engineering hit by two data breaches., from *Reuters.com*: http://www.reuters.com/article/2015/05/15/pennstate-dataprotection-idUSL3N0Y66KK20150515

McCarthy, K. (2015, January 15). 5 colleges with data breaches larger than Sony's in 2014. Retrieved 07 11, 2015, from Huffingtonpost.com: http://www.huffingtonpost.com/kyle-mccarthy/five-colleges-with-data-b_b_6474800.html

O'Neil, M. (2014, March 17). Data breaches put a dent in colleges' finances as well as reputations. *The Chronical of Higher Education.* http://chronicle.com/article/Data-Breaches-Put-a-Dent-in/145341/

Roman, J. (2014, June 30). Add Butler University to breach list - Latest incident highlights breach vulnerabilities in academia. from *DataBreachToday.com*: http://www.databreachtoday.com/add-butler-university-to-breach-list-a-7007

Straumshein, C. (2015, July 06). A Playground for Hackers. from *Inside Higher Ed*: https://www.insidehighered.com/news/2015/07/06/pennsylvania-state-u-cyberattacks-possibly-part-larger-trend-experts-say

Svitek, P., & Anderson, N. (2014, February 19). University of Maryland computer security breach exposes 300,000 records. from *WashingtonPost.com*: http://www.washingtonpost.com/local/college-park-shady-grove-campuses-affected-by-university-of-maryland-security-breach/2014/02/19/ce438108-99bd-11e3-80ac-63a8ba7f7942_story.html